UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/053,139	01/21/2002	Pierre De Lanauze	SWA-3.2.017/4286	4800

26345 7590 10/12/2005

GIBBONS, DEL DEO, DOLAN, GRIFFINGER & VECCHIONE
1 RIVERFRONT PLAZA
NEWARK, NJ 07102-5497

EXAMINER	
HERRING, VIRGIL A	
ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 10/12/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 10/053,139	**Applicant(s)** DE LANAUZE, PIERRE	
	Examiner Virgil Herring	**Art Unit** 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 January 2002*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)□ Claim(s) _____ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-32* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *1/21/02* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

This action is responsive to the communication filed on 21 January 2002. Claims 1-32, representing a method and apparatus for secure encryption using biometrics, are pending. Claims 1-32 are rejected.

Drawings

The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they include the following reference character(s) not mentioned in the description: 73, 74.

The descriptions provided for steps 72 and 92a do not match the figures to which they refer.

The specification refers to a step of converting the fingerprint image to gray scale. In figure 1, it is shown as "grey" scale.

Corrected drawing sheets in compliance with 37 CFR 1.121(d), or amendment to the specification to add the reference character(s) in the description in compliance with 37 CFR 1.121(b) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Specification

The disclosure is objected to because of the following informalities:

IBS should be defined the first time it is used on page 4, rather than on page 10 after it has been used 19 times.

ASIC should also be defined on page 6 where it is first used.

On page 15, in paragraph 45, the applicant states, "For this reason, in step 52b only the IBS (which sensors the cryptographic key) is generated." The examiner suspects that "sensors" is not the right word for this sentence, and requests clarification.

Appropriate correction is required.

Claim Objections

IBS should be defined the first time it is used on page 22 of the claims.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 2-13, 29, and 31-32 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 2 recites the limitation "the step of generating," but is unclear which step of generating is being referenced.

Claim 2 also recites the limitation "...wherein the step of generating is performed using a secret algorithm..." This does not particularly point out or distinctly claim the process by which the cryptographic key is being generated, as required by 3 U.S.C. 112.

Claim 3 recites the limitation "the encryption key" in line 1. There is insufficient antecedent basis for this limitation in the claim.

Claim 4 recites the limitation "the step of extracting" in line 1. There is insufficient antecedent basis for this limitation in the claim.

Claim 6 recites the limitation "the step of deriving" in line 3. There is insufficient antecedent basis for this limitation in the claim.

Claim 11 recites the limitation "the step of generating," but is unclear which step of generating is being referenced.

Claim 12 recites the limitation "the step of generating," but is unclear which step of generating is being referenced.

Claim 29 recites the limitation "the message" in line 7 of page 27. There is insufficient antecedent basis for this limitation in the claim.

Claim 31 recites the limitations "the IBS" and "the sender" in lines 3-5. There is insufficient antecedent basis for these limitations in the claim.

Claims 5, 7-10, 13, and 32 are rejected based on their dependency on one or more of the previously rejected claims.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-3, 14-17, 20-22, and 30-31 are rejected under 35 U.S.C. 102(b) as being anticipated by Bjorn (398).

With respect to claim 1, Bjorn (398) discloses a method for generating a cryptographic key, comprising steps of:

using a sensor to acquire an image of a biometric feature of a user; (Col. 3, Lines 26-27)

generating binary output from analog signals output by the sensor; and (Col. 3, Lines 34-35)

generating the cryptographic key from the binary output using a selection algorithm. (Col. 3, Lines 54-56)

Bjorn (398) describes how features are extracted from an analog scan of a fingerprint, and those features are used to build a template of the fingerprint. This template is then hashed. In different embodiments, this hash may be either the cryptographic key itself, or used as the basis for generating a key. Because these actions take place in a computer system (Bjorn Figure 1), those skilled in the art would recognize that any data stored would be in a binary format.

With regards to claim 20, Bjorn (398) discloses an apparatus for generating a cryptographic key comprising a sensor system adapted to:

capture an image of a biometric feature of a user; and (Col. 3, Lines 26-27)

extract from the image an identity bit string (IBS) used to generate the cryptographic key. (Col. 3, Lines 34-35)

Bjorn (398) describes the way in which fingerprints are handled. First, features are extracted from the analog image, and used to build a template. Because this occurs in a computer system, those skilled in the art will recognize that this template must be a bit string that identifies the person to whom the associated fingerprint belongs. Bjorn later describes several ways in which this identifying string of bits can be used to generate a cryptographic key.

In examining claim 2, the examiner has assumed that "the step of generating" refers to the step of "generating the cryptographic key from the binary output using a selection algorithm." With respect to claims 2 and 21, Bjorn (398) discloses a method as claimed in claim 1 wherein the step of generating is performed using a secret algorithm for selecting, arranging, and performing operations on the binary output. (Col. 3, Lines 44-47 & 57-58)

Bjorn (398) discloses the use of a hash function (specifically MD5) to convert a digital representation of a fingerprint to a cryptographic key. "Selecting, arranging, and performing operations on" a binary string are known in the art as steps in the MD5 hash algorithm.

In examining claim 3, the examiner has assumed that "the encryption key" should read "the cryptographic key." With respect to claims 3 and 22, Bjorn (398) discloses a method as claimed in claim 2 wherein the encryption key is a key for a private key cryptographic system. (Col. 4, Lines 40-41)

With respect to claim 30, Bjorn (398) discloses a method for encrypting a message addressed to a user comprising a step of applying an encryption algorithm to the message using an encryption key derived from binary output generated from an analog signal associated with an image of a biometric feature of the user. (Col. 3, Lines 56-57)

Bjorn (398) discloses the generation of a cryptographic key based on a user's fingerprint. It is inherent that a cryptographic key will be used for the encryption or decryption of data. It is also inherent that to perform such encryption or decryption, an appropriate encryption or decryption algorithm must be applied to the message.

With respect to claim 14, Bjorn (398) discloses an apparatus for decrypting an encrypted message addressed to a user, the apparatus comprising a processor adapted to use an IBS derived from an image of a biometric feature of the user in conjunction with a decryption algorithm to decrypt the encrypted message. (Col. 1, Lines 40-43; Col. 3, Lines 54-56; Col. 4, Lines 38-46)

With respect to claim 15, Bjorn (398) discloses an apparatus as claimed in claim 14 wherein the processor is adapted to use the IBS as a cryptographic key to decrypt the message using the decryption algorithm. (Col. 4, Lines 40-43)

With respect to claim 16, Bjorn (398) discloses an apparatus as claimed in claim 15 wherein the processor is further adapted to first authenticate the user by matching the IBS with a reference bit string prior to decrypting the message. (Col. 5, Lines 3-6)

With respect to claim 17, Bjorn (398) discloses an apparatus as claimed in claim 14 wherein the processor is further adapted to:

use the IBS to authenticate the user, by matching the IBS with a reference bit string associated with the user; (Col. 5, Lines 3-6) if the user is authenticated, apply a transformation algorithm to the IBS in order to generate a cryptographic key; and (Col. 3, Lines 56-57)

decrypt the message using the cryptographic key and a decryption algorithm. (Col. 4, Lines 40-43)

With respect to claim 31, Bjorn (398) discloses a method as claimed in claim 30 further comprising a step of:

authenticating the user by comparing the IBS with a reference bit string uniquely associated with the sender. (Col. 4, Lines 60-62)

The use of fingerprints to identify a person is widely known. The use of an identifying bit string that represents a fingerprint is no different from analog methods of doing so, because in both cases comparisons are made regarding locations of various features (whorls, ridge endpoints, etc.).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 18, 19, and 32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bjorn (398) in view of Lang (429).

With respect to claim 18, Bjorn does not expressly disclose an apparatus as claimed in claim 17 wherein the processor resides on a smart card that stores the transformation algorithm, the decryption algorithm, and the reference bit string.

However, Lang (429) discloses a system in which the user is supplied with a smart card and identification codes, which uses biometric information for extremely secure applications. The user must enter an access code to a card reading device to attempt to access secured information (Col. 3, Lines 64-66). The smart card contains additional codes used to access this information (Col. 4, Lines 1-3). Bjorn and Lang are analogous art because both deal with the protection of data using biometrics. To apply the teachings of Lang to Bjorn, one would use a fingerprint scanner connected with the card reader to input the ID code to the smart card. This could be accomplished either by creating Bjorn's fingerprint template in the card reader, or transferring the fingerprint image to the smart card and creating the template there. Bjorn discloses that there known methods for a processor to compare the template to verify the user's identity (Bjorn, Col. 5, Lines 4-6). This would require the processor (now residing on the smart card) to contain a reference template. The smart card would contain the decryption algorithm (Lang, Col. 3, Lines 28-30). The processor is capable of generating a key from a fixed-length hash of the template (Bjorn, Col. 3, Lines 56-57). This would inherently require the use of some sort of transformation algorithm. The motivation for combining Bjorn and Lang would have been to provide a personal accessing device to allow access to secured information while not being constrained by location.

With respect to claim 19, Bjorn (398) does not expressly disclose an apparatus as claimed in claim 18 wherein the smart card is docked at a card reader adapted to interface with both a sensor system, from which the IBS is received, and a communications processor from which the message is received.

However, the combination of Bjorn (398) with Lang (429) as described above includes a card reader interfaced with a fingerprint sensor, which can generate a template of a fingerprint (IBS). It is inherent that the card reader would also have to be connected to a communications processor, because the message being encrypted or decrypted is not generated by the smart card or the card reader, but rather, by another user in a public or private key security system (Bjorn, Col. 4, Lines 40-43).

With regards to claim 32, Bjorn (398) does not expressly disclose a method as claimed in claim 31, further comprising a step of inserting a smart card into a card reader, the card reader being adapted to convey the IBS to the smart card.

However, Lang (429) discloses the use of smart cards in a biometric-based cryptographic system. In column 3, lines 62-64, Lang (429) discloses the use of contact and contactless smart card readers. Those skilled in the art would recognize that the use of some types of contact smart card reader would necessitate the insertion of a suitable smart card. Smart cards are typically small enough for a user to carry them around, and are thus too small for all the equipment required for scanning a fingerprint. Thus, the fingerprint scanner must inherently be separate from the smart card. Because the scanner is a key component in the generation of a fingerprint template (Bjorn), the template creation process cannot be part of the smart card. Thus, the template (IBS) must be communicated to the smart card, using the card reader. The motivation for combining Bjorn with the teachings of Lang would have been to provide a personal accessing device to allow access to secured information while not requiring the user to be in a specific place.

Claims 4,7, 23, and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bjorn (398) in view of Schmitt et al (225).

In examining claim 4, the examiner has assumed that "the step of extracting" refers to the step of generating binary output from analog signals. With respect to claim 4 Bjorn (398) fails to disclose a method as claimed in claim 3 wherein the step of extracting comprises steps of:

receiving the image in an analog signal format;

passing the analog signal through an analog filter to remove gray scale from the analog signal; and converting the filtered analog signal to a binary output signal.

However, Schmitt et al (225) disclose the conversion of a gray scale fingerprint image to a binarized fingerprint image using a binarizing filter (Col. 8, Lines 64-67). Bjorn (398) and Schmitt et al (225) are analogous art because both deal with the use of fingerprints in security. At the time of the invention, it would have been obvious to one skilled in the art to convert an analog image of a fingerprint to a binary image. The motivation for doing so would have been to provide dynamic image contrast enhancement, which would result in reduced computational requirements later in the identification process (Schmitt et al, Col. 9, Lines 1-2, 8-10). To apply the teachings of Schmitt et al (225) to Bjorn (398), one would therefore include a binarizing filter between the fingerprint sensor and whatever processor is controlling the generation of the cryptographic key.

With respect to claim 23, Bjorn (398) discloses an apparatus as claimed in claim 21 wherein the sensor system further comprises a sensor for generating an analog signal representative of the image of the biometric feature (Col. 3, Lines 6-7). Bjorn (398) fails to disclose an apparatus as claimed in claim 21 wherein the integrated circuit further comprises:

an analog filter adapted to eliminate gray scale from the analog signal;

a converter adapted to convert the filtered analog signal to binary output;

and

a selection algorithm adapted to extract the IBS from the binary output.

However, Schmitt et al (225) disclose the use of a binarizing filter to convert a gray scale fingerprint image to a binary representation (Col. 8, Lines 64-67). Bjorn (398) and Schmitt et al (225) are analogous art because both patents use fingerprints in security. At the time of the invention, it would have been obvious to include the binarizing filter from Schmitt et al (225) in the cryptographic key generator of Bjorn (398). The motivation for doing so would have been to provide dynamic image contrast enhancement, which would result in reduced computational requirements later in the process (Schmitt et al, Col. 9, Lines 1-2, 8-10).

With respect to claims 7 and 26, the combination of Bjorn (398) and Schmitt et al (225) discloses a method as claimed in claim 4 or 23 wherein the cryptographic key is derived from values extracted from the binary output that are unrelated to information used to classify or identify the biometric feature, so that the information cannot be used to associate the cryptographic key with the biometric feature. (Bjorn, Col. 3, Lines 61-65)

Bjorn (398) discloses the generation of ghost points in a template of a fingerprint. Because the ghost points are randomly placed on the fingerprint image, they are not associated with any identifying feature of the fingerprint. In figure 5 and in column 6-7, Bjorn explains the process of key generation using the ghost points. When the template is created, extra points are added in random locations to signify features that are not present in the actual fingerprint. Thus, the template cannot be used to identify the fingerprint, or the person to whom it belongs, because there is no way to tell which of the points are real and which are not. When the user wants to generate a key, the fingerprint is scanned and the measured features are subtracted from the template, leaving only the ghost points. The template of ghost points is then hashed to create a key that is in no way related to the fingerprint.

Claims 5-6 and 24-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bjorn (398) in view of Schmitt et al (225) and further in view of McMahon (462).

With respect to claim 5, the combination of Bjorn (398) and Schmitt et al (225) does not disclose a method as claimed in claim 4 wherein the step of using a sensor comprises steps of:

receiving electromagnetic radiation from the biometric feature at a charge coupled device; and

acquiring an image of the biometric feature.

However, McMahon (462) discloses the use of a 32x32 array of charge coupled silicon light detectors in scanning a fingerprint pattern (Col. 13, Lines 28-32). Light is a form of electromagnetic radiation, and silicon light detectors are devices. Bjorn (398), Schmitt et al (225), and McMahon are analogous art because they all deal with the use of fingerprints in security arrangements. At the time of the invention, it would have been obvious to use an array of charge coupled silicon light detectors to scan a fingerprint in the generation of a cryptographic key. The motivation for doing so would have been to take advantage of the high quantum efficiency and sensitivity to infrared light of a charge coupled device.

With respect to claim 24, the combination of Bjorn (398) and Schmitt et al (225) does not expressly disclose an apparatus as claimed in claim 23 wherein the sensor comprises a charge coupled device (CCD) adapted to generate the analog signal in response to electromagnetic radiation, and the biometric feature comprises a predefined surface area of a user's body.

However, McMahon (462) discloses the use of a 32x32 array of charge coupled silicon light detectors in scanning a fingerprint pattern (Col. 13, Lines 28-32). It is inherent that a fingerprint is a predefined surface area of a person's body. Bjorn (398), Schmitt et al (225), and McMahon are analogous art because they are all related to the topic of fingerprint scanning. At the time of the invention, it would have been obvious to one skilled in the art to use an array of charge coupled silicon light detectors to scan a fingerprint for the purpose of cryptographic key generation. The motivation for doing so would have been to utilize the naturally high quantum efficiency and sensitivity to infrared light of a charge coupled device.

With respect to claim 6, the combination of Bjorn (398), Schmitt et al (225) and McMahon (462) discloses a method as claimed in claim 5 wherein the biometric feature is a pattern located on a predefined surface area of a body and the step of deriving further comprises an initial step of measuring a life sign indicator of the surface area of the body in order to verify that the image is of a living being. (Schmitt et al, Col. 10, Lines 5-8)

A fingerprint is a pattern located on a predefined surface area of a body. Schmitt et al (225) discloses the use of impedance sensors to verify that the object being scanned is a living finger. The motivation to include this would have been to prevent "spoofing" of the system using a finger removed from its owner.

With respect to claim 25, the combination of Bjorn (398), Schmitt et al (225) and McMahon (462) discloses an apparatus as claimed in claim 24 wherein the sensor is adapted to capture an image of a fingerprint, and the sensor area further comprises means for acquiring at least one measurement indicating that a finger placed on the sensor area is the finger of a living being. (Schmitt et al, Col. 10, Lines 5-8)

Claims 8-13 and 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bjorn (398) in view of Schmitt et al (225) and further in view of Lang (429).

With respect to claim 8, the combination of Bjorn (398) with Schmitt et al (225) does not disclose a method as claimed in claim 4 further comprising a step of forwarding an IBS to a processor that stores a decryption algorithm for use with the cryptographic key to decrypt messages addressed to the user.

However, Lang (429) discloses an electronic document security system in which a user inputs an identification code to a smart card (Col. 3, Lines 11-14) that contains an encryption/decryption algorithm (Col. 3, Lines 28-31). It is known in the art that a smart card is a processor attached to a card for portability. Though Lang does not specifically disclose that the identification code is a bit string, those skilled in the art will recognize that a bit string is merely one way of representing a series of letters or numbers. Bjorn, Schmitt et al, and Lang are analogous art because they deal with methods of encryption and decryption of data involving biometrics. At the time of the invention, it would have been obvious to one skilled in the art that a processor such as a smart card would be capable of receiving an identification code, such as an IBS, and that such a card could also store a decryption algorithm. The motivation to include this would have been to allow a user to access encrypted information, while maintaining protection from unauthorized access to the data (Lang, Col. 2, Lines 35-41).

In examining claim 11, the examiner has assumed that "the step of generating" refers to the step of "generating the cryptographic key" of claim 1. With respect to claim 11, the combination of Bjorn (398), Schmitt et al (225), and Lang (429) as described above includes a method as claimed in claim 8 wherein the step of generating is performed by the processor, and comprises steps of:

receiving the IBS; and

applying a transformation algorithm to the IBS to generate the cryptographic key.

It is inherent that if the IBS were forwarded to the processor in claim 8, then the processor would receive it. Bjorn (398) discloses the use of MD5 in converting the image of a fingerprint to a numerical representation, and using that hash as a basis for generating a cryptographic key (Col. 3, Lines 54-58). Known algorithms for generating a cryptographic key include mathematical and logical steps to transform data from its original form to a different form.

With respect to claims 9 and 12, the combination of Bjorn (398), Schmitt et al (225), and Lang (429) as previously described covers a method as claimed in claim 8 wherein the processor has access to a decryption algorithm that uses the IBS as the cryptographic key, and the method further comprises a step of using the IBS to authenticate the user by determining if the IBS matches a reference bit string, prior to decrypting the message.

It is an inherent property of processors that they have access to data they store, because otherwise they would have no function. This would include a situation in which a processor stores a decryption algorithm. Lang (429) discloses the use of the identification code, which is transmitted to the processor on the smart card, to verify the identity of the user (Col. 3, Lines 11-13). The examiner interprets Lang's phrase "...correctly enter his personal identification code..." to mean that if the code is entered incorrectly the process is aborted. Comparing the entered code to a stored copy of the code to see if they match is the traditional method for performing this verification. As seen in Bjorn, a bit string generated from a fingerprint can be used as a cryptographic key.

With respect to claims 10 and 13, the combination of Bjorn (398), Schmitt et al (225), and Lang (429) covers a method as claimed in claim 9 wherein the processor resides on a smart card, and the method further comprises an initial step of inserting the smart card into a card reader that is adapted to receive both the message and the IBS.

Lang (429) discloses the use of a contact smart card reader (Col. 3, Lines 62-64). Contact smart card readers typically operate by inserting the card in a slot on the reading device or placing the card against the reading device. Because a smart card is typically too small to include all the components necessary to construct a fingerprint scanner, those skilled in the art would recognize that the scanner would be external to the smart card, either as a part of the card reader, or a device connected to the card reader. Because this is the case, the scanner must inherently include a method for communicating with the fingerprint scanner or IBS generator.

With respect to claim 27, the combination of Bjorn (398), Schmitt et al (225), and Lang (429) described previously covers an apparatus as claimed in claim 23 wherein the integrated circuit comprises:

a circuit for generating an IBS by selecting, arranging, and performing operations on values obtained from the binary output using a predefined selection algorithm; and

a circuit for sending the IBS to a processor.

Bjorn (398) discloses the use of MD5 as a step in converting the image of a fingerprint to create a cryptographic key. MD5 is a hash algorithm that transforms data using steps of selecting, arranging, and performing operations on the data in a predefined order. It is known in the computing art that an algorithm such as MD5 requires a circuit on which to execute, typically in the form of an ALU. Lang (429) discloses the use of a smart card that contains an encryption/decryption algorithm and is capable of receiving a user identification code. He also discloses the use of a contactless smart card, in which the identification code is entered to a separate device, and communicated to the processor in the smart card (Col. 3-4, Lines 61-68, 1-3).

With respect to claim 28, the combination of Bjorn (398), Schmitt et al (225), and Lang (429) as described above includes an apparatus as claimed in claim 27 wherein the processor is further adapted to generate the cryptographic key from the IBS by applying a transformation algorithm to the IBS.

Bjorn (398) discloses the generation of a cryptographic key from a hash of an image of a fingerprint (Col. 3, Lines 54-58). Known algorithms for generation of cryptographic keys include logical and mathematical steps to transform data from one form to another.

With respect to claim 29, the combination of Bjorn (398), Schmitt et al (225) and Lang (429) as described above includes an apparatus as claimed in claim 28 wherein the processor resides on a smart card, and the apparatus further comprises a card reader, the smart card being adapted to:

receive the IBS from the integrated circuit, via the card reader; (Lang, Col. 3, Lines 64-66, where the identification code is a binarized representation of the user's fingerprint, as shown in Schmitt et al)

determine if the IBS matches a reference bit string associated with the user, to authenticate the user; (Lang, Col. 3, Lines 11-13)

if the user is authenticated, apply the transformation algorithm to the IBS to generate the cryptographic key; and (Bjorn, Col. 3, Lines 56-57)

apply a decryption algorithm to the message using the cryptographic key. (Lang, Col. 3, Lines 28-31)

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Virgil Herring whose telephone number is (571) 272-8189. The examiner can normally be reached on Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Virgil Herring
Examiner
Art Unit 2132

VAH

Gilberto

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100